1. Record Nr. UNINA9910483434903321

Titolo	Advances in Cryptology – EUROCRYPT 2015 : 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part II / / edited by Elisabeth Oswald, Marc Fischlin
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2015
ISBN	3-662-46803-4
Edizione	[1st ed. 2015.]
Descrizione fisica	1 online resource (XVIII, 838 p. 102 illus.)
Collana	Security and Cryptology ; ; 9057
Disciplina	005.82
Soggetti	Data encryption (Computer science) Algorithms Computer security Management information systems Computer science Cryptology Algorithm Analysis and Problem Complexity Systems and Data Security Management of Computing and Information Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Universal Signature Aggregators -- Fully Structure-Preserving Signatures and Shrinking Commitments -- Disjunctions for Hash Proof Systems: New Constructions and Applications -- Quasi-Adaptive NIZK for Linear Subspaces Revisited -- Leakage-Resilient Circuits Revisited – Optimal Number of Computing Components Without Leak-Free Hardware -- Noisy Leakage -- Privacy-Free Garbled Circuits with Applications to Efficient Zero-Knowledge -- Two Halves Make a Whole: Reducing Data Transfer in Garbled Circuits Using Half Gates -- One-Out-of-Many Proofs: Or How to Leak a Secret and Spend a Coin -- The Bitcoin Backbone Protocol: Analysis and Applications -- Linear Secret Sharing Schemes from Error Correcting Codes -- Function Secret Sharing -- Cluster Computing in Zero Knowledge -- Hosting Services

on an Untrusted Cloud -- How to Obfuscate Programs Directly -- Cryptographic Agents: Towards a Unified Theory of Computing on Encrypted Data -- Executable Proofs, Input-Size Hiding Secure Computation and a New Ideal World -- Semantically Secure Order-Revealing Encryption: Multi-input Functional Encryption Without Obfuscation -- Improved Dual System ABE in Prime-Order Groups via Predicate Encodings -- Resisting Randomness Subversion: Fast Deterministic and Hedged Public-Key Encryption in the Standard Model -- Cryptographic Reverse Firewalls -- Mind the Gap: Modular Machine-Checked Proofs of One-Round Key Exchange Protocols -- Authenticated Key Exchange from Ideal Lattices -- Non-Interactive Zero-Knowledge Proofs in the Quantum Random Oracle Model -- Privacy Amplification in the Isolated Qubits Model -- Generic Hardness of the Multiple Discrete Logarithm Problem.

Sommario/riassunto

The two-volume proceedings LNCS 9056 + 9057 constitutes the proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2015, held in Sofia, Bulgaria, in April 2015. The 57 full papers included in these volumes were carefully reviewed and selected from 194 submissions. The papers are organized in topical sections named: honorable mentions, random number generators, number field sieve, algorithmic cryptanalysis, symmetric cryptanalysis, hash functions, evaluation implementation, masking, fully homomorphic encryption, related-key attacks, fully monomorphic encryption, efficient two-party protocols, symmetric cryptanalysis, lattices, signatures, zero-knowledge proofs, leakage-resilient cryptography, garbled circuits, crypto currencies, secret sharing, outsourcing computations, obfuscation and e-voting, multi-party computations, encryption, resistant protocols, key exchange, quantum cryptography, and discrete logarithms.